ID: 289647
Sample Name: PRODUCT LIST _IMG.exe
Cookbook: default.jbs
Time: 17:45:48
Date: 24/09/2020
Version: 30.0.0 Red Diamond

Table of Contents

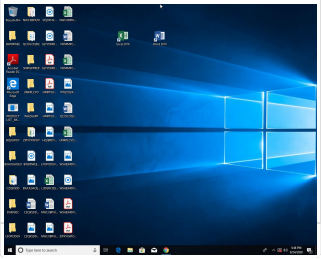
Analysis Report PRODUCT LIST _IMG.exe

Overview

General Information

Sample Name:	PRODUCT LIST _IMG.exe
Analysis ID:	289647
MD5:	9a28fb8644f6c94..
SHA1:	bda74e1af9c7d63.
SHA256:	bc7988fcd34bc5f...
Tags:	exe

Most interesting Screenshot:



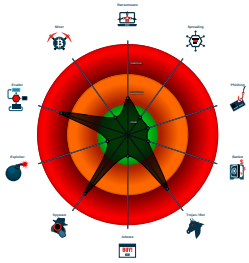
Detection

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- .NET source code contains very larg…
- Allocates memory in foreign process…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect virtualization through…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- PRODUCT LIST _IMG.exe (PID: 6480 cmdline: 'C:\Users\user\Desktop\PRODUCT LIST _IMG.exe' MD5: 9A28FB8644F6C9413772F5BB0D41E2F0)
  - RegAsm.exe (PID: 3128 cmdline: C:\Users\user\AppData\Local\Temp\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.512025324.000000000699 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000003.511720075.000000000699 4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.637339151.000000000018 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000003.513888831.000000000699 5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000003.511687221.000000000699 4000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

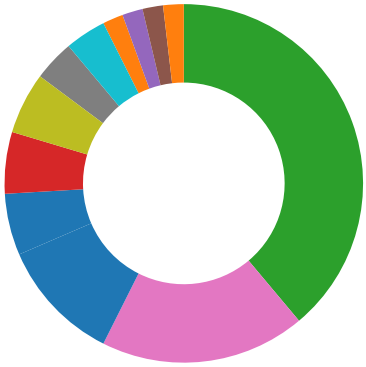
Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.RegAsm.exe.180000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

System Summary:

- .NET source code contains very large array initializations
- Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

- Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

- Allocates memory in foreign processes

Stealing of Sensitive Information:

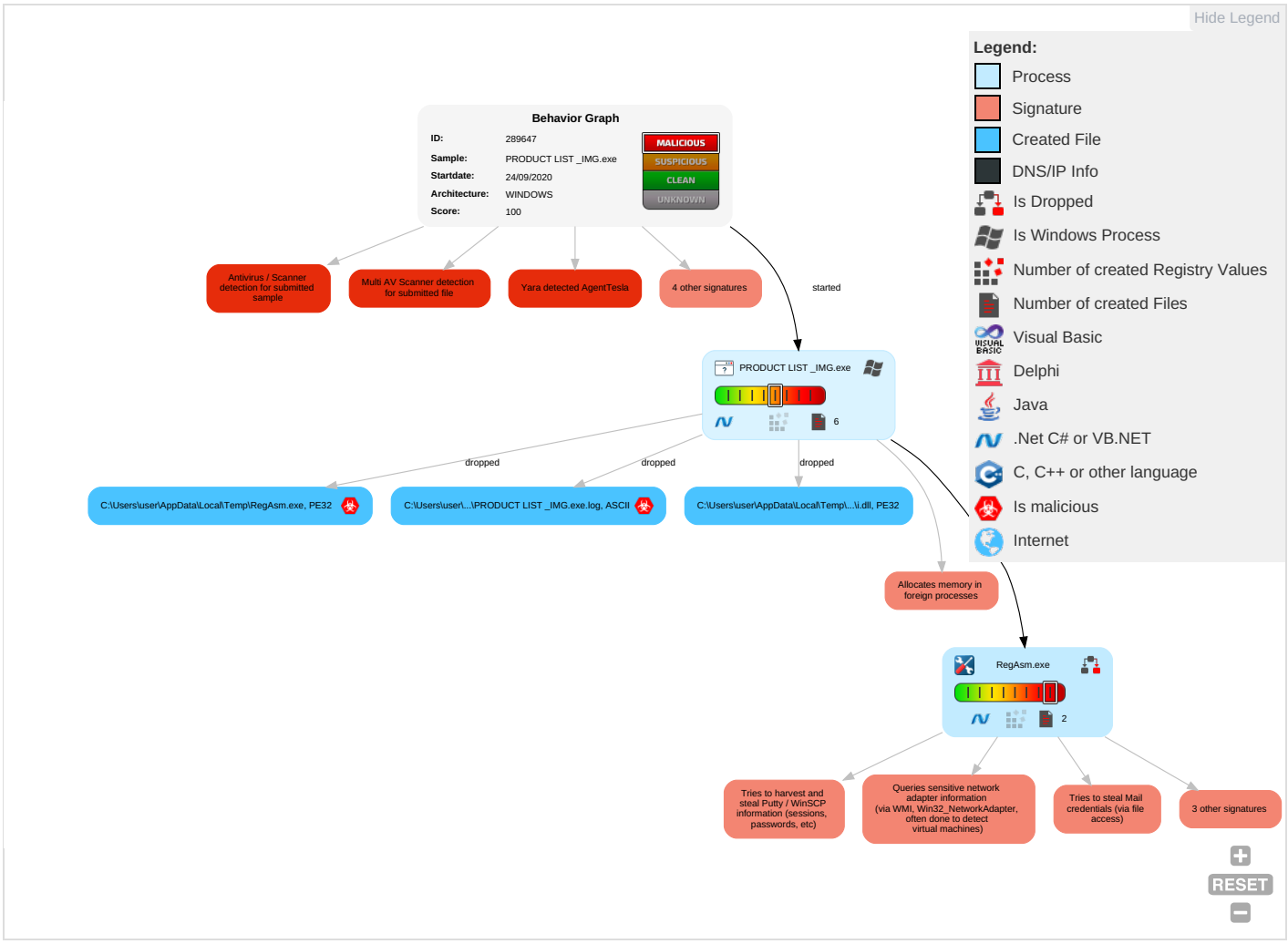
- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to harvest and steal ftp login credentials
- Tries to steal Mail credentials (via file access)

Remote Access Functionality:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping 2	Security Software Discovery 2 1 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 3	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	System Information Discovery 2 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

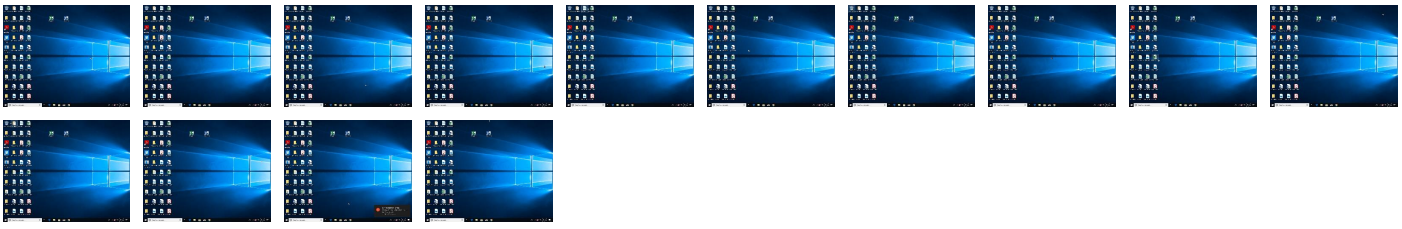
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PRODUCT LIST _IMG.exe	33%	Virustotal		Browse
PRODUCT LIST _IMG.exe	23%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
PRODUCT LIST _IMG.exe	100%	Avira	HEUR/AGEN.1122384	
PRODUCT LIST _IMG.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\b1f92ac9-345d-4ee6-83d6-512dab76f3b9\i.dll	3%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.PRODUCT LIST _IMG.exe.460000.0.unpack	100%	Avira	HEUR/AGEN.1122384		Download File
0.2.PRODUCT LIST _IMG.exe.460000.0.unpack	100%	Avira	HEUR/AGEN.1122384		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ns.adobe.c	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://ocsp.thawte.com0	0%	URL Reputation	safe	
http://VNgxdn.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.telegra	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 0000000B.00000002.638876591.0000000002381000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram.org/bot1322270726:AAE8ex2tDrvB9GA6y4VV0psQLtRL4yhRDdo/	RegAsm.exe, 0000000B.00000002.637339151.0000000000182000.00000040.00000001.sdmp	false		high
http://DynDns.comDynDNS	RegAsm.exe, 0000000B.00000002.638876591.0000000002381000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.thawte.com/ThawteTimestampingCA.crl0	i.dll.0.dr	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 0000000B.00000002.638876591.0000000002381000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.symauth.com/rpa00	i.dll.0.dr	false		high
http://ns.adobe.c	PRODUCT LIST _IMG.exe, 00000000.00000003.428873431.0000000061B9000.00000004.00000001.sdmp, PRODUCT LIST _IMG.exe, 00000000.00000003.428941437.0000000061B9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.thawte.com0	i.dll.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://VNgxdn.com	RegAsm.exe, 0000000B.00000002.638876591.0000000002381000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1322270726:AAE8ex2tDrvB9GA6y4VV0psQLtRL4yhRDdo/sendDocumentdocument-----	RegAsm.exe, 0000000B.00000002.638876591.0000000002381000.00000004.00000001.sdmp	false		high
http://www.symauth.com/cps0(	i.dll.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PRODUCT LIST _IMG.exe, 00000000.00000003.509049844.000000000062EB000.00000004.00000001.sdmp, RegAsm.exe, 0000000B.00000002.637339151.0000000000182000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	RegAsm.exe, 0000000B.00000002.638876591.0000000002381000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegra	PRODUCT LIST _IMG.exe, 00000000.00000003.509049844.000000000062EB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	30.0.0 Red Diamond
Analysis ID:	289647
Start date:	24.09.2020
Start time:	17:45:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PRODUCT LIST _IMG.exe
Cookbook file name:	default.jbs
Analysis system description:	w10x64 Windows 10 64 bit v1803 with Office Professional Plus 2016, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.3% (good quality ratio 0.8%) • Quality average: 16.5% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, UsoClient.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:46:41	API Interceptor	249x Sleep call for process: PRODUCT LIST _IMG.exe modified
17:47:53	API Interceptor	388x Sleep call for process: RegAsm.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\b1f92ac9-345d-4ee6-83d6-512dab76f3b9\i.dll	SecuriteInfo.com.FileRepMalware.exe	Get hash	malicious	Browse	
	Encomenda Fornecedor n#U00ba 72718_____PDF.exe	Get hash	malicious	Browse	
	summary.exe	Get hash	malicious	Browse	
	Quote N city 6oct Modification...exe	Get hash	malicious	Browse	
	PDF4567823.exe	Get hash	malicious	Browse	
	Kovetes reszletei.exe	Get hash	malicious	Browse	
	Quotation Request for Urgent Shipment - Minimum order Quantity and Fastest Lead time REF22002.exe	Get hash	malicious	Browse	
	MELAG QUOTATION 0095986.exe	Get hash	malicious	Browse	
	AMD129 Spec Request for Quotation and Fastest Shipping Time - ref21092020 00933.exe	Get hash	malicious	Browse	
	URGENT QUOTATION.exe	Get hash	malicious	Browse	
	Draft Ship Documents GB00033312TT 240HQFOBUV99034080 - JJFL70010066 - DQ-277 ETD 25 Sep.exe	Get hash	malicious	Browse	
	REQUEST FOR PRODUCTS SUPPLY.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.1220.18568.exe	Get hash	malicious	Browse	
	Shipment documents for Order 20TDD67 440HQ BLMYRH BL009676 ContainerSKIU3444367221.exe	Get hash	malicious	Browse	
	DHL Shipment Arrival Notice AWB 5406506482.xlsx	Get hash	malicious	Browse	
	PO-074-20-DM4.exe	Get hash	malicious	Browse	
	FedEx's AWB#5305323204643.exe	Get hash	malicious	Browse	
	September Payment -Bank Details.exe	Get hash	malicious	Browse	
	talent.exe	Get hash	malicious	Browse	
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\RegAsm.exe	SecuriteInfo.com.FileRepMalware.exe	Get hash	malicious	Browse	
	Utn3pm8rDY.exe	Get hash	malicious	Browse	
	Anast_red.exe	Get hash	malicious	Browse	
	Anast_redlinecs.exe	Get hash	malicious	Browse	
	RFQ#F44E0741.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.ArtemisA5D28505F884.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Fareit-FVT95F44C3806B1.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Quote best price of 75000pcsPO.exe	Get hash	malicious	Browse	
	PO.exe	Get hash	malicious	Browse	
	Outstanding_payment202047654.arj.exe	Get hash	malicious	Browse	
	ProductServices Enquiry.exe	Get hash	malicious	Browse	
	FACTURA_FISCALA-RO81061402-6403840980_(31-Aug-20)_PDF.exe	Get hash	malicious	Browse	
	G_ZEVELEKAKIS_ORDER3108_PDF.exe	Get hash	malicious	Browse	
	ORDER_310800312PDF.exe	Get hash	malicious	Browse	
	ORDER#5944395-pdf.exe	Get hash	malicious	Browse	
	ORDER#49532001-pdf.exe	Get hash	malicious	Browse	
	proforma invoice.exe	Get hash	malicious	Browse	
	SOA and SES numbers PDF.exe	Get hash	malicious	Browse	
	Machine PO3742020.exe	Get hash	malicious	Browse	
	RRRRRR.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT LIST _IMG.exe.log	
Process:	C:\Users\user\Desktop\PRODUCT LIST _IMG.exe
File Type:	ASCII text, with CRLF line terminators
Size (bytes):	1976
Entropy (8bit):	5.3569395659576475
Encrypted:	false
MD5:	D1F580650522B7EBD7F438FD6B22F339
SHA1:	768BA6465A6C6107AC504EC2E254F090021EB643
SHA-256:	8280C0A16B5638C762196E6C892BF0940FF9C94435407C66992DA9D592999910
SHA-512:	BE90D7CD9009EF4BB5DE65E64CE522CBEFE3070386D937CCEACFB85E949CA39F954DD5808593D1A4FB806E990E61D465E83B87B80CD2540CF1CE80A0B1847(0C
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\PRODUCT LIST _IMG.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070(
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Joe Sandbox View:	• Filename: SecuriteInfo.com.FileRepMalware.exe, Detection: malicious, Browse • Filename: Utn3pm8rDY.exe, Detection: malicious, Browse • Filename: Anast_red.exe, Detection: malicious, Browse • Filename: Anast_redlinecs.exe, Detection: malicious, Browse • Filename: RFQ#F44E0741.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.ArtemisA5D28505F884.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Fareit-FVT95F44C3806B1.exe, Detection: malicious, Browse • Filename: Quote best price of 75000pcsPO.exe, Detection: malicious, Browse • Filename: PO.exe, Detection: malicious, Browse • Filename: Outstanding_payment202047654.arj.exe, Detection: malicious, Browse • Filename: ProductServices Enquiry.exe, Detection: malicious, Browse • Filename: FACTURA_FISCALA-RO81061402-6403840980_(31-Aug-20)_PDF.exe, Detection: malicious, Browse • Filename: G_ZEVELEKAKIS_ORDER3108_PDF.exe, Detection: malicious, Browse • Filename: ORDER_310800312PDF.exe, Detection: malicious, Browse • Filename: ORDER#5944395-pdf.exe, Detection: malicious, Browse • Filename: ORDER#49532001-pdf.exe, Detection: malicious, Browse • Filename: proforma invoice.exe, Detection: malicious, Browse • Filename: SOA and SES numbers PDF.exe, Detection: malicious, Browse • Filename: Machine PO3742020.exe, Detection: malicious, Browse • Filename: RRRRRR.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o..... .*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o .....r]..p.o!....,.{T.....{U.....o"....+(.ra..p.o!....,.{T.....

C:\Users\user\AppData\Local\Temp\b1f92ac9-345d-4ee6-83d6-512dab76f3b9\i.dll	
Process:	C:\Users\user\Desktop\PRODUCT LIST _IMG.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Size (bytes):	96664
Entropy (8bit):	5.567444078679915
Encrypted:	false
MD5:	14FF402962AD21B78AE0B4C43CD1F194
SHA1:	F8A510EB26666E875A5BDD1CADAD40602763AD72
SHA-256:	FB9646CB956945BDC503E69645F6B5316D3826B780D3C36738D6B944E884D15B
SHA-512:	DAA7A08BF3709119A944BCE28F6EBDD24E54A22B18CD9F86A87873E958DF121A3881DCDD5E162F6B4E543238C7AEF20F657C9830DF01D4C79290F7C9A4FCC5B
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 3%
Joe Sandbox View:	• Filename: SecuriteInfo.com.FileRepMalware.exe, Detection: malicious, Browse • Filename: Encomenda Fornecedor n#U00ba 72718_____PDF.exe, Detection: malicious, Browse • Filename: summary.exe, Detection: malicious, Browse • Filename: Quote N city 6oct Modification...exe, Detection: malicious, Browse • Filename: PDF4567823.exe, Detection: malicious, Browse • Filename: Kovetes reszletei.exe, Detection: malicious, Browse • Filename: Quotation Request for Urgent Shipment - Minimum order Quantity and Fastest Lead time REF22002.exe, Detection: malicious, Browse • Filename: MELAG QUOTATION 0095986.exe, Detection: malicious, Browse • Filename: AMD129 Spec Request for Quotation and Fastest Shipping Time - ref21092020 00933.exe, Detection: malicious, Browse • Filename: URGENT QUOTATION.exe, Detection: malicious, Browse • Filename: Draft Ship Documents GB00033312TT 240HQFOBUV99034080 - JJFL70010066 - DQ-277 ETD 25 Sep.exe, Detection: malicious, Browse • Filename: REQUEST FOR PRODUCTS SUPPLY.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Inject4.1220.18568.exe, Detection: malicious, Browse • Filename: Shipment documents for Order 20TDD67 440HQ BLMYRHBL009676 ContainerSKIU3444367221.exe, Detection: malicious, Browse • Filename: DHL Shipment Arrival Notice AWB 5406506482.xlsx, Detection: malicious, Browse • Filename: PO-074-20-DM4.exe, Detection: malicious, Browse • Filename: FedEx's AWB#5305323204643.exe, Detection: malicious, Browse • Filename: September Payment -Bank Details.exe, Detection: malicious, Browse • Filename: talent.exe, Detection: malicious, Browse • Filename: FedExs AWB#5305323204643.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....jr..jr..jr..8...ir.....kr.....cr..jr..9r..8...kr.....sr.....kr....x.kr..jr..kr..... kr..Richjr.....PE..L...5 .\.....!.....F.....0.....Z.....@.....C.....0b..d.....b.....4...`A..8.....x7..@..... .....`..0....p..`.....text...h..... ..`.rdata.....0....."....@..@.data.....P.....:.....@....idata.....`.....<.....@..@.didat..a....p.....J..... ..@....00cfg.....N.....@..@.rsrc.....P.....@..@.reloc.....X.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

General

Entropy (8bit):	7.365437710257741
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PRODUCT LIST _IMG.exe
File size:	405504
MD5:	9a28fb8644f6c9413772f5bb0d41e2f0
SHA1:	bda74e1af9c7d634647fe4aacab9baf628f5a6bb
SHA256:	bc7988fcd34bc5f8313b980f83197c4e9e41437097e8911e2744388ad026bd1a
SHA512:	07a93f9d57fae29bef76c68c8433e241708cc58e6763adfa621a568a972ba608b5c31ced901df85779ab407925bd8232f340314731 17fd1b80221fec0e14e23e
SSDEEP:	6144:ROnJca2zaKj1EkoZ4OKLCCtMOzC0eEqYjAC8J:RqiqKjsZ4OM3MOehEqgiJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....^.....0..&.....D... ..`....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4644ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5EA08F02 [Wed Apr 22 18:37:54 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x64480	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x66000	0x4f6	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x68000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x624d4	0x62600	False	0.679327648507	data	7.38245937622	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x66000	0x4f6	0x600	False	0.387369791667	data	3.87040823571	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x68000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x660a0	0x26c	data		
RT_MANIFEST	0x6630c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	0.0.0.0
InternalName	PRODUCT LIST _IMG.exe
FileVersion	0.0.0.0
ProductVersion	0.0.0.0
FileDescription	
OriginalFilename	PRODUCT LIST _IMG.exe

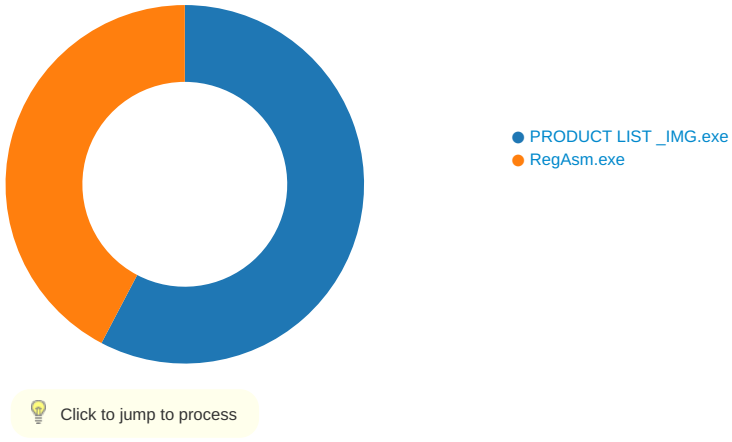
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PRODUCT LIST _IMG.exe PID: 6480 Parent PID: 6096

General

Start time:	17:46:40
Start date:	24/09/2020
Path:	C:\Users\user\Desktop\PRODUCT LIST _IMG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PRODUCT LIST _IMG.exe'
Imagebase:	0x460000
File size:	405504 bytes
MD5 hash:	9A28FB8644F6C9413772F5BB0D41E2F0

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.512025324.0000000006995000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.511720075.0000000006994000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.513888831.0000000006995000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.511687221.0000000006994000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.512281428.0000000006995000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.510897867.000000000698C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000003.506497242.00000000062DD000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E28CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E28CF06	unknown
C:\Users\user\AppData\Local\Temp\b1f92ac9-345d-4ee6-83d6-512dab76f3b9	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D0DBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\b1f92ac9-345d-4ee6-83d6-512dab76f3b9\i.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D0D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\RegAsm.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	E2DBA9	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT LIST _IMG.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E59C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\b1f92ac9-345d-4ee6-83d6-512dab76f3b9\i.dll	unknown	96664	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2e 13 e9 ef 6a 72 87 bc 6a 72 87 bc 6a 72 87 bc 38 1a 82 bd 69 72 87 bc 05 16 83 bd 6b 72 87 bc 05 16 86 bd 63 72 87 bc 6a 72 86 bc 39 72 87 bc 38 1a 84 bd 6b 72 87 bc e5 1b 82 bd 73 72 87 bc e5 1b 87 bd 6b 72 87 bc e5 1b 78 bc 6b 72 87 bc 6a 72 10 bc 6b 72 87 bc e5 1b 85 bd 6b 72 87 bc 52 69 63 68 6a 72 87 bc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $...........jr..jr..jr..8...ir ......kr......cr..jr..9r..8... kr......sr......kr....x.kr..jr ..kr......kr..Richjr.......... ........PE..L..	success or wait	1	6D0D1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0	64616	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 78 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b0 00 00 00 0c 00 00 00 00 00 00 5e ce 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 df c9 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...xX.Z.......... ....0............^.... ....@.. ....`.................	success or wait	1	E2DBA9	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PRODUCT LIST_IMG.exe.log	unknown	1976	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=	success or wait	1	6E59C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E265705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E26CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E1C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6E265705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll	unknown	523400	success or wait	1	7349B80F	ReadFile

Analysis Process: RegAsm.exe PID: 3128 Parent PID: 6480

General

Start time:	17:47:42
Start date:	24/09/2020
Path:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\RegAsm.exe
Imagebase:	0xa0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.637339151.0000000000182000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.639005721.0000000002402000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E28CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E28CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E265705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E1C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	1	6E26CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E26CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E1C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4097	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4098	success or wait	2	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	7976	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4121	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4253	success or wait	1	6E265705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E265705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E1C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E1C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	2	6D0D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D0D1B4F	ReadFile

Disassembly

Code Analysis